UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,428	04/05/2006	Olivier Brique	90500-000035/US	2506

30593   7590   12/10/2008
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER
WRIGHT, BRYAN F

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/517,428	BRIQUE ET AL.
Office Action Summary	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>22 August 2008</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>17-35</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>17-35</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>8/22/2008</u>.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

FINAL ACTION

1.   Claims 17-35 are pending.

Claim Rejections - 35 USC § 102

        The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2.   Claims 17-35 are rejected under 35 U.S.C. 102(b) as being anticipated by Hardy

et al. (EP 0 537971 BA and Hardy hereinafter (cited from IDS)).

3.   As to claim 17, Hardy teaches a data exchange method between two devices

locally connected to one another (i.e., teaches a communication link between first and

second terminal [col. 3, lines 15-20]), especially between a security module and a

receiver (i.e., .. teaches a terminal having the ability to encrypted (e.g., secure)

message,) the first device comprising at least one first encrypting key of a pair of

asymmetric keys and the second device comprising at least the second encrypting key

of said pair of asymmetric keys (i.e., ...teaches a each secure terminal contain a pair of

key management database [col. 4, lines 50-55] ... further teaches one for encrypting

and another for decrypting [col. 4, lines 50-55]), these keys being previously initialised in

the first and second device (i.e., .. .teaches terminal device maintains the a key

database), this method comprising:

- generating, at least one first random number in the first device (i.e., … teaches generating a random number [col., 6, lines 40-50]), - generating, at least one second random number in the second device (i.e., … teaches generating a random number [col., 6, lines 40-50] …further teaches a random number is generated in each terminal [col. 7, lines 1-5]), - encrypting said first random number by said first encrypting key (i.e., …teaches encrypting random number [col. 6, lines 40-50]), - encrypting said second random number by said second encrypting key (i.e., …teaches encrypting random number [col. 6, lines 40-50]), - transmitting said first encrypted random number to the second device (i.e., … teaches random component message exchange [col. 6, lines 45-55]), - transmitting said second encrypted random number to the first device [col. 6, lines 45-55], - decrypting the first encrypted random number in said second device (i.e., …teaches the message is process using a public key to decrypt the message [col. 6, lines 55-58]) , - decrypting the second encrypted random number in said first device [col. 7, lines 10-15], - combining said random numbers generated by one of the devices and received by the other device to generate a session key (e.g., traffic key) (i.e., … teaches combining the random to produce a third random used as a traffic key [col. 7, lines 15-25]), - and using the session key (i.e., traffic key) to encrypt and decrypt all or part of the exchanged data between the first and second device (i.e., .. teaches using the traffic key as part of a key generation process for cryptographic process between terminals [col., 7, lines 20-35]).

4.   As to claim 18, Hardy teaches a data exchange method random number (i.e.,

seed), generated by the first device and decrypted by the second device - is encrypted

by said second device by means of said second encrypting key, - is transmitted in a

encrypted form to said first device, - is decrypted in this first device by means of the first

encrypting key and - is compared to said random number generated by the first device,

and wherein the data transfer is stopped if the compared random numbers are not

identical (i.e., …teaches a comparison made between received decrypted encrypted

seed and check data pattern with stored version. ... further teaches communication

synchronization is dependent on a match [col. 7, lines 50-58 - col. 8, lines 1-5]).

5.   As to claim 19, Hardy teaches a data exchange method where the random

number (i.e., seed), generated by the second device and decrypted by the first device -

is encrypted by said first device by means of said first encrypting key, - is transmitted in

a encrypted form to said second device, - is decrypted in this second device by means

of the second encrypting key and - is compared to said random number generated by

the second device, and wherein the data transfer is stopped if the compared random

numbers are not identical (i.e., …teaches a comparison made between received

decrypted encrypted seed and check data pattern with stored version. ... further

teaches communication synchronization is dependent on a match [col. 7, lines 50-58 -

col. 8, lines 1-5]).

6.   As to claim 20, Hardy teaches a data exchange method in which said first device

and said second device contain a symmetric encrypting key, wherein the random

numbers are combined with said symmetric key to generate a session key (i.e., ...

teaches combining the random to produce a third random used as a traffic key [col. 7,

lines 15-25] ... further teaches using the traffic key as part of a key generation process

for cryptographic process between terminals [col., 7, lines 20-35]).

7.   As to claim 21, Hardy teaches a data exchange method where the combination

of said random numbers is a concatenation [col. 9, lines 45-55].

8.   As to claim 22, Hardy teaches a data exchange method where the combination

of said random numbers is a concatenation [col. 9, lines 45-55].

9.   As to claim 23, Hardy teaches a data exchange method where the session key

(i.e., traffic key) is regenerated in function of a determined parameter of use (i.e., ...

teaches the traffic key is use as a parameter to a key generation process for

cryptographic purposes [col. 7, lines 20-35]).

10.   As to claim 24, Hardy teaches a data exchange method where the determined

parameter of use is the duration of use [col. 7, lines 20-35]).

11.   As to claim 25, Hardy teaches a data exchange method where at least one of the
two devices measures at least one representative physical parameter of the
communication (i.e., teaches a communication link between first and second terminal
[col. 3, lines 15-20]), such as the line impedance and/or the electric consumption,
wherein one compares the values measured to the reference values, and wherein one
acts on the data exchange when the measured parameters differ from the reference
values more than a threshold value (pre-determined number) [col. 9, lines 25-35]).

12.   As to claim 26, Hardy teaches a data exchange method where one acts by
stopping the data exchange between the two devices [col. 9, lines 25-35]).

13.   As to claim 27, Hardy teaches a data exchange method where the session key
(i.e., traffic key) is regenerated in function of a determined parameter of use and
wherein the determined parameter of use is the representative physical parameter of
the communication (i.e., ... teaches generating a traffic key by combining two random
number such that the random number [col. 9, lines 35- 58]).

14.   As to claim 28, Hardy teaches a data exchange method where - at least one of
the devices generates at least one supplementary random number (i.e., ... teach a
random number is generated in each terminal [col. 7, lines 1-5], - this supplementary
random number is encrypted by said first encrypting key [col. 7, lines 1-5] , - this
supplementary encrypted random number is transmitted to the second device [col. 7,

lines 1-5], - this transmitted encrypted supplementary random number is decrypted in

this second device [col. 7, lines 10-15], - the decrypted supplementary random number

is encrypted by said second encrypting key (i.e., ... teaches a seed and pattern data is

encrypted [col. 10, lines 1-5], - the supplementary encrypted random number is

transmitted to the first device (i.e., ...teaches transmission of data [col. 10, lines 5-10], -

the supplementary random number decrypted in the first device is compared to the

initial supplementary random number generated in said first device (i.e., ... teaches

decrypting and comparing data [col. 10, lines 5-15]), - the information exchange is

interrupted if the comparison indicates that the two compared numbers are not identical

(i.e., ...teaches terminating communication if failure [col. 9, lines 30-36]).

15.   As to claim 29, Hardy teaches a data exchange method where - at least one of

the devices determines at least one predefined fixed number memorized (i.e., third

random number generated from combining to two random number) in the two devices

[col. 9, lines 50-58], - this predefined fixed number is encrypted by said first encrypting

key, - this predefined fixed encrypted number is transmitted to the second device [col.

10, lines 1-5], - this transmitted encrypted predefined fixed number is decrypted in this

second device [col. 10, lines 5-10], - the predefined fixed number decrypted in the

second device is compared to the predefined fixed number memorized in this second

device [col. 10, lines 11- 16], - the data exchange is interrupted if the comparison

indicates that the two compared numbers are not identical [col. 9, lines 30-36].

16.   As to claim 30, Hardy teaches a data exchange method according where each of

the numbers is encrypted separately [col. 9, lines 38-41].

17.   As to claim 31, Hardy teaches a data exchange method where each of the

numbers is encrypted separately [col. 9, lines 38-41].

18.   As to claim 32, Hardy teaches a data exchange method where a combination of

each of the numbers is encrypted [col. 9, lines 40-50].

19.   As to claim 33, Hardy teaches a data exchange method where a combination of

each of the numbers is encrypted [col. 9, lines 40-50].

20.   As to claim 34, Hardy teaches a receiver for carrying out the method, this

receiver comprising at least one calculation unit, a read-only memory, a demultiplexer, a

descrambler, a digital/analog converter, an external memory and a sound and image

descrambler, wherein at least the calculation unit, the read-only memory and the

descrambler are contained in a same electronic chip and wherein at least one of the

encrypting keys is stored in said electronic chip (i.e., .. .teaches a microcontroller

technology [fig. 6] ... further teaches telephone network communication [fig. 1]).

21.   As to claim 35, Hardy teaches a receiver where at least one of the numbers (i.e.,

first number) is stored in said electronic chip (e.g., terminal) (i.e., ... teaches first

random number stored in original terminal [col. 7, lines 10-15]).

Response to Arguments

Applicant's arguments, see Amendment/Req. Reconsideration, filed 8/22/2008,

with respect to the rejection(s) of claim(s) 17-35 have been fully considered and are

persuasive. Therefore, the rejection has been withdrawn. However, upon further

consideration, a new ground(s) of rejection is made in view of Hardy et al. (EP 0 537971

BA) The new grounds was prompted by IDS filed by applicant on 8/22/2008. As a

result of this filing and applicant paying the fee, this action is made FINAL.

Conclusion

Applicant's submission of an information disclosure statement under 37 CFR

1.97(c) with the fee set forth in 37 CFR 1.17(p) on 8/22/2008 prompted the new

ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS

MADE FINAL**. See MPEP § 609.04(b). Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-

3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system. Status information for
published applications may be obtained from either Private PAIR or Public PAIR.
Status information for unpublished applications is available through Private PAIR only.
For more information about the PAIR system, see http://pair-direct.uspto.gov. Should
you have questions on access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a
USPTO Customer Service Representative or access to the automated information
system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431
                              /Kimyen Vu/
              Supervisory Patent Examiner, Art Unit 2435